

**(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international**



(43) Date de la publication internationale
11 janvier 2001 (11.01.2001)

(10) Numéro de publication internationale
WO 01/02955 A1

(51) Classification internationale des brevets⁷: G06F 9/45

(21) Numéro de la demande internationale: PCT/FR00/01815

(22) Date de dépôt international: 28 juin 2000 (28.06.2000)

(25) Langue de dépôt: français

(26) Langue de publication: français

(30) **Données relatives à la priorité:**
99/08460 1 juillet 1999 (01.07.1999) FR

(71) **Déposants** (*pour tous les États désignés sauf US*):
BULL CP8 [FR/FR]; 68, route de Versailles, f-78430

Louvenciennes (FR). INSTITUT NATIONAL DE LA RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE [FR/FR]; Domaine de Voluceau, Rocquencourt, F-78153 Le Chesnay Cedex (FR). CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE (CNR S) [FR/FR]; 3, rue Michel-Ange, F-75794 Paris Cedex 16 (FR).

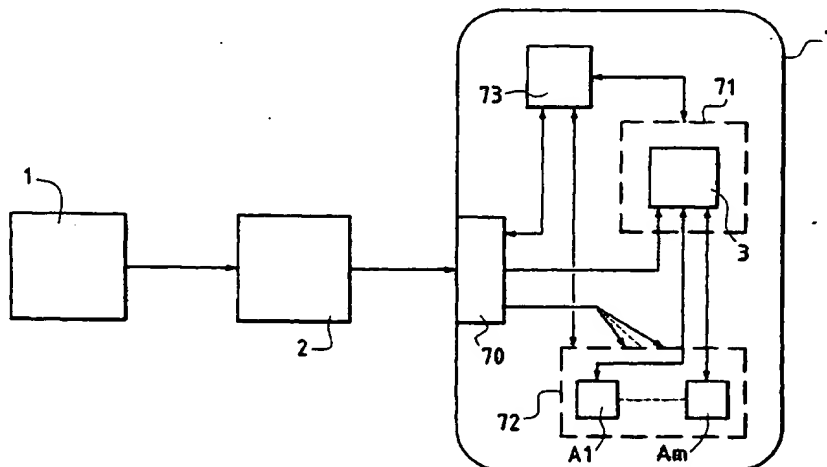
(72) Inventeurs; et

(75) **Inventeurs/Déposants** (*pour US seulement*): **GOIRE, Christian** [FR/FR]; 8, allée du Mail, F-78340 Les Clayes-sous-Bois (FR). **JENSEN, Thomas** [FR/FR]; IRISA/INRIA, Campus Universitaire de Beaulieu, F-35042 Rennes Cedex (FR). **FRADET, Pascal** [FR/FR]; IRISA/INRIA, Campus Universitaire de Beaulieu, F-35042 Rennes Cedex (FR). **LE METAYER, Daniel** [FR/FR]; IRISA/INRIA, Campus Universitaire de Beaulieu, F-35042

[Suite sur la page suivante]

(54) Title: METHOD FOR VERIFYING CODE TRANSFORMERS FOR AN INCORPORATED SYSTEM, IN PARTICULAR IN A CHIP CARD

(54) Titre: PROCÉDE DE VERIFICATION DE TRANSFORMATEURS DE CODES POUR UN SYSTEME EMBARQUE, NOTAMMENT SUR UNE CARTE A PUCE



(S7) Abstract: The invention concerns a method for verifying a transformer of source code into a transformed code designed for an incorporated system (7). The method comprises at least steps which consist in: determining a single virtual machine factoring the behaviour of said two codes (1, 3); determining for each of said source (1) and transformed (3) codes a plurality of functions called auxiliary functions representing residual differences between said source (1) and transformed (3) codes; and a step which consists in verifying a property of correspondence between the auxiliary functions, the code transformer (2) verification resulting from the latter step. The invention is particularly applicable to chip cards (7).

[Suite sur la page suivante]

BEST AVAILABLE COPY

WO 01/02955 A1



Rennes Cedex (FR). DENNEY, Ewen [FR/FR]; IRISA/INRIA, Campus Universitaire de Beaulieu, F-35042 Rennes Cedex (FR).

Publiée:

— Avec rapport de recherche internationale.

(74) Mandataire: ROGER PETIT, Georges; Office Bletry, 94, rue Saint Lazare, F-75010 Paris (FR).

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(81) États désignés (*national*): BR, CA, CN, JP, US.

(84) États désignés (*régional*): brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

(57) **Abrégé:** L'invention concerne un procédé de vérification d'un transformateur de code source en un code transformé destiné à un système embarqué (7). Le procédé comprend au moins les étapes de détermination d'une machine virtuelle unique factorisant le comportement de ces deux codes (1, 3), la détermination, pour chacun desdits codes source (1) et transformé (3), d'une pluralité de fonctions dites auxiliaires représentant des différences résiduelles entre lesdits codes source (1) et transformé (3) et une étape consistant à vérifier une propriété de correspondance entre les fonctions auxiliaires, la vérification du transformateur de code (2) étant obtenue à partir de cette dernière étape. Application notamment aux cartes à puce (7).

PROCÉDÉ DE VÉRIFICATION DE TRANSFORMATEURS DE CODES POUR UN SYSTÈME EMBARQUÉ, NOTAMMENT SUR UNE CARTE À PUCE

L'invention concerne un procédé de vérification de transformateurs de codes pour un système embarqué.

L'invention concerne aussi l'application d'un tel procédé à un transformateur pour générer un code destiné à une carte à puce.

5 Dans le cadre de l'invention, le terme "système embarqué" doit être considéré dans son acception la plus générale. Il concerne notamment des systèmes destinés à une carte à puce, ce qui constitue l'application préférée de l'invention, mais également tout système destiné à un dispositif portable ou mobile comportant des moyens propres de traitement de données informatisés,
10 que l'on appellera ci-après "ressources de traitement".

Les systèmes embarqués modernes sont munis de ressources de traitement des données permettent de remplir des fonctions de plus en plus complexes et de plus en plus nombreuses. Cependant, malgré la mise sur le marché de technologies et de composants de plus en plus performants, une
15 caractéristique distinctive des systèmes embarqués, par rapport à des systèmes informatiques conventionnels (micro-ordinateur, station de travail, etc.), concerne les limitations qu'ils imposent en matière de ressources (taille mémoire et puissance des microprocesseurs notamment). Pour satisfaire ces contraintes, il est nécessaire de transformer le code destiné à être exécuté sur
20 un système embarqué. Les transformations ont pour but de produire un code plus efficace et plus économe en ressources.

Pour fixer les idées, et à titre d'exemple non limitatif de code, on considérera dans ce qui suit un programme écrit dans la machine virtuelle du langage "JAVA" (marque déposée par SUN MICROSYSTEMS) qui présente
25 l'intérêt de pouvoir être exécuté dans de nombreux environnements. Les domaines d'application de ce langage se sont en effet multipliés notamment avec le développement important du réseau Internet. De nombreuses applications logicielles de petite taille, dites "applets", sont écrites dans ce langage et exécutables par un navigateur de type "WEB"

2

On se placera également dans le cadre de l'application préférée de l'invention, à savoir l'exécution d'un code de ce type par les ressources informatiques propres d'une carte à puce. Comme il a été rappelé ci-dessus, malgré des progrès technologiques importants, la capacité mémoire de la carte à puce, ainsi que la puissance du microprocesseur qui l'équipe restent relativement limités. Il est également important que le code soit résident dans la carte à puce, car les transmissions entre celle-ci et un terminal hôte, quel qu'il soit, s'effectuent à basse vitesse. Les standards actuels ne prévoient que des transmissions de type série. Le besoin se fait donc sentir de disposer d'un code que l'on pourrait qualifier "d'allégé", en tout cas optimisé pour cet usage. Pour ce faire, il a été proposé d'utiliser un langage dérivé de "JAVA", se présentant sous la forme d'une restriction de ce langage, à savoir le langage "JAVA CARD" (marque déposée également par SUN MICROSYSTEMS).

Une complication supplémentaire vient du fait que les systèmes embarqués sont généralement utilisés dans des environnements qui requièrent les plus hautes garanties en matière, à la fois de fiabilité et de sécurité. On peut citer à titre d'exemple les nouvelles versions de cartes à puce sur lesquelles on souhaite installer des applications logicielles multiples qui doivent coopérer harmonieusement sans révéler d'informations confidentielles. En effet, *a priori*, ces multiples applications peuvent concerner des utilisateurs distincts. Malgré la coopération précitée, on doit conserver un cloisonnement rigoureux, pour que les informations concernant un utilisateur donné restent confidentielles, pour le moins ne puissent pas être mises à la disposition d'un utilisateur non habilité à les connaître (lecture) et/ou à les manipuler (écriture et opérations connexes : effacement, modification). En dehors de l'aspect "confidentialité", d'autres exigences sont à prendre en compte, notamment l'exigence dite "d'intégrité" : pertes de données, modifications non conformes, etc.

Si on considère le code "source", dans le sens de "code initial", tel que par exemple le "byte code" du langage "JAVA" précité, ce dernier présente toutes les garanties nécessaires et remplit les exigences précitées, le "byte code" étant un programme écrit dans la machine virtuelle du langage "JAVA".

3

En effet, de nombreux tests ont pu être effectués, ce pendant de longues périodes de temps.

Le code dit "transformé" est obtenu à partir du "code source" à l'aide d'un transformateur de code, généralement extérieur au système embarqué, mais qui peut également être résident dans celui-ci. Il est donc nécessaire de
5 montrer l'équivalence entre le code source et le code transformé.

Cela peut s'effectuer en garantissant que les transformations effectuées sur le code ne changent en rien son comportement (d'un point de vue externe) et n'introduisent pas de failles de sécurité. En d'autres termes, le
10 code initial (avant transformation) doit être d'un point de vue logique équivalent au code résultant (après transformation).

Il est particulièrement difficile de garantir cette propriété en général, car les transformations ont un effet global sur le code et sur les représentations des données qu'il manipule. De façon pratique, la complexité impliquée par
15 cette opération ne permet pas une mise en œuvre dans des conditions économiques et/ou technologiques réalistes. En outre, on doit bien comprendre que de tels besoins ne sont apparus que très récemment, notamment en conjonction avec le développement des technologies précitées de cartes à puce multi-applications et/ou multi-utilisateurs.

20 L'invention vise à répondre à ces besoins, sans nécessiter des procédures extrêmement longues et coûteuses.

Le procédé selon l'invention permet de vérifier de manière systématique et modulaire la correction des transformations de codes.

Dans le cadre de l'invention, deux formalismes, bien connus en soi, seront utilisés de façon essentielle : les sémantiques opérationnelles et les
25 relations logiques. Pour une description plus détaillée de ces formalismes, on se reportera avec profit, pour le premier, au livre de : H. R. Nielson, et F. Nielson, intitulé : "*Semantics with Applications: A formal Introduction*". Wiley, 1992, et, pour le second, au livre de J. Mitchell : "*Foundations for Programming
30 Languages*", MIT Press, 1996.

Selon une caractéristique essentielle de l'invention, le procédé de vérification des transformateurs de codes consiste à spécifier le sens de deux

4

codes à l'aide d'une machine virtuelle commune paramétrée par des fonctions que l'on appellera "fonctions auxiliaires". Les différences entre les deux codes sont exprimées et regroupées dans les fonctions auxiliaires précitées. Chaque fonction auxiliaire possède deux versions : une version dans le code source et
5 une version dans le code transformé. Les premiers modules étant identiques, puisque communs aux deux codes, il n'y a pas lieu de vérifier s'ils sont équivalents. Pour montrer l'équivalence des deux codes, il suffit donc de montrer que les fonctions dites auxiliaires, considérées deux à deux, sont équivalentes. Ces deux sous-ensembles peuvent être rendus beaucoup moins
10 complexes que les deux ensembles représentés par les deux codes, source et transformé, considérés dans leur intégralité. Il s'ensuit que, selon le procédé de l'invention, la difficulté inhérente au processus de vérification est très fortement réduite, et de façon corrélative, le processus de vérification devient économiquement et technologiquement réalisable.

15 L'invention a donc pour objet un procédé de vérification d'un transformateur de code dit source en un code dit transformé destiné à un système embarqué, lesdits codes source et transformé étant associés à des machines virtuelles, caractérisé en ce qu'il comprend au moins les étapes suivantes :

- 20 - la détermination, pour chacun desdits codes source et transformé, d'un premier sous-ensemble commun, constituant une machine virtuelle unique factorisant le comportement de ces deux codes ;
- la détermination, pour chacun desdits codes source et transformé, d'un second sous-ensemble constitué d'une pluralité de fonctions dites
25 auxiliaires, lesdites fonctions auxiliaires représentant des différences résiduelles entre lesdits codes source et transformé ;
- l'association par paire desdites fonctions auxiliaires, une première fonction auxiliaire de chaque paire appartenant audit second sous-ensemble associé audit code source et une seconde fonction auxiliaire de chaque
30 paire appartenant audit second sous-ensemble associé audit code transformé ;

5

- la vérification d'une propriété de correspondance déterminée entre lesdites fonctions auxiliaires de toutes lesdites paires ; et
- la vérification que ladite transformation du code source en code transformé par ledit convertisseur respecte ladite propriété de correspondance déterminée.

L'invention a encore pour objet l'application d'un tel procédé à un transformateur pour la génération d'un code destiné à être enregistré dans une carte à puce.

L'invention va maintenant être décrite de façon plus détaillée en se référant aux dessins annexés, parmi lesquels :

- la figure 1 illustre schématiquement le processus de transformation d'un code source en un code transformé final ;
- les figures 2A et 2B illustrent schématiquement une des caractéristiques essentielles du procédé selon l'invention ; et
- la figure 3 illustre schématiquement l'application du procédé selon l'invention à une carte à puce ;

On va maintenant décrire de façon détaillée le procédé de vérification de transformateurs de codes selon l'invention.

La figure 1 illustre schématiquement le processus de transformation d'un code 1, que l'on appellera "code source", dans le sens de code origine ou initial, en un code final 3, dit "code transformé", à l'aide d'un transformateur de code 2. Ce dernier organe peut être un moyen informatique ou une pièce de logiciel spécifique. De façon habituelle, le code transformé est destiné à être résident dans le système embarqué 4 (en trait plein). Le transformateur 2 peut également être résident ou téléchargé dans le système embarqué : référence 4' (en traits pointillés).

Après chargement ou enregistrement dans le système embarqué 4-4', le code transformé 3 permet l'exécution d'une ou plusieurs tâches en tant que de besoin, représentées sous la référence unique 5. On suppose que le système embarqué 4 dispose de ressources informatiques autonomes classiques (non représentées).

6

A priori, la transformation de code est effectuée une fois pour toutes par un transformateur donné 2 ou dans de rares occasions : modification de version du code d'origine ou code source 1, par exemple.

Il est donc nécessaire que l'on puisse établir la preuve formelle que le code transformé 3 est équivalent au code source 1. Ce processus permet de vérifier si le transformateur 2 fonctionne de façon correcte.

Cependant, comme il a été rappelé, si on considère, dans leur globalité, les deux ensembles formés par les codes, source et transformé, la théorie montre qu'une telle détermination n'est généralement pas possible de façon réaliste.

Une caractéristique essentielle du procédé selon l'invention va consister à trouver pour chacun des deux codes deux sous-ensembles, que l'on appellera premier et second sous-ensembles. Selon une caractéristique importante du procédé selon l'invention, les premiers sous-ensembles forment une machine virtuelle commune aux deux codes, source et transformé. De ce fait, il n'est donc pas nécessaire de vérifier l'équivalence des premiers sous-ensembles.

Les seconds sous-ensembles, constitués des fonctions auxiliaires, sont par contre distincts d'un code à l'autre. La détermination de l'équivalence des codes, source et transformé, se réduit alors à la détermination de l'équivalence de toutes les paires de fonctions auxiliaires des seconds sous-ensembles. Or, la complexité résiduelle des fonctions auxiliaires peut être très réduite. Il s'ensuit que la détermination d'équivalence précitée devient possible.

Les figures 2A et 2B illustrent très schématiquement le procédé selon l'invention.

Comme le montre plus particulièrement la figure 2A, les premiers sous-ensembles du code source 1 et du code transformé 3 forment une machine virtuelle commune 13. Les seconds sous-ensembles, 10 et 30, sont constitués chacun par une série de fonctions dites auxiliaires, dont l'équivalence devra être vérifiée. Ces fonctions auxiliaires, 10 et 30, paramètrent la machine virtuelle commune 13.

7

L'équivalence des deux codes, source 1 et transformé 2, se réduit donc à vérifier l'équivalence des fonctions auxiliaires, 10 et 30, prises deux à deux, comme il le sera montré ci-après en regard de la figure 2B.

5 Les étapes du procédé vont maintenant être décrites de façon plus détaillée.

Les codes source et transformé sont associés à des première et seconde machines dites virtuelles, respectivement.

10 La première étape consiste en la définition d'une machine virtuelle (ou sémantique opérationnelle) unique permettant de factoriser le comportement du code source et du code transformé. Les différences entre les deux codes apparaissent alors à travers des fonctions auxiliaires qui seront interprétées ou mises en oeuvre différemment dans les deux codes.

Une machine virtuelle peut se représenter par un ensemble de règles de la forme :

15

prémisse 1

.

.

.

20

prémisse n

état1[Instruction1] \Rightarrow état2

(1).

25 Les prémisses sont, soit des conditions d'application d'une règle, c'est-à-dire des expressions booléennes, soit des affectations à des variables utilisées pour exprimer un changement d'état. Les prémisses font appel à des fonctions auxiliaires pour extraire des informations de l'état ou exprimer des conditions. Chaque règle indique comment l'état de la machine évolue lorsque les prémisses sont vérifiées et l'instruction "Instruction1" est rencontrée. On 30 définit une ou plusieurs règles de cette forme pour chaque type d'instruction du code.

8

La seconde étape consiste en la définition de types ou structures de données utilisés dans les deux codes. On définit des types basiques comme, par exemple :

5 Basique ::= Nat | Bool | Nom... (2),

et des types construits comme, par exemple :

 Environnement ::= Nom → Valeur
10 Instructions ::= Instruction1 | Instruction2 | ... (3),

La troisième étape consiste en l'interprétation de types, référencés θ , utilisés dans les machines virtuelles. Pour chaque type θ , on définit une interprétation pour le code source $\llbracket \theta \rrbracket_s$ et une interprétation pour le code transformé, $\llbracket \theta \rrbracket_t$, plus une relation R_θ entre les deux interprétations $\llbracket \cdot \rrbracket_s$ et $\llbracket \cdot \rrbracket_t$. Ces relations, appelées relations logiques, respectent la structure des types. Pour des types simples, elles doivent être définies explicitement ; pour des types structurés, elles sont déduites des types des composants de la structure.

20 Par exemple, pour les paires :

$$(a, b) R_{\theta_1 \times \theta_2} (a', b') \Leftrightarrow a R_{\theta_1} a' \wedge b R_{\theta_2} b' \quad (4),$$

relation dans laquelle θ_1 et θ_2 sont des types et a, b, a' et b' des éléments de type.

Il en est de même pour les fonctions :

$$f R_{\theta_1 \rightarrow \theta_2} f' \Leftrightarrow \forall a, a'. a R_{\theta_1} a' \Rightarrow f a R_{\theta_2} f' a' \quad (5).$$

30 Les relations logiques doivent être la relation "identité" pour les types observables, c'est à dire des types pour lesquels on veut montrer que les deux

9

codes rendent le même résultat. Il s'agit habituellement de types imprimables et/ou affichables sur un écran informatique. Cela peut être des types basiques, mais également des types structurés représentant, par exemple, une pile ou des variables d'un programme donné.

5 La quatrième étape consiste en l'interprétation des fonctions auxiliaires utilisées dans les machines virtuelles. Pour chaque fonction auxiliaire f , on donne sa définition pour le code source, notée $\llbracket f \rrbracket_s$, et sa définition pour le code transformé, notée $\llbracket f \rrbracket_r$.

10 La détermination de l'équivalence consiste à montrer que les définitions des fonctions auxiliaires respectent les relations logiques. Plus précisément, pour chaque fonction auxiliaire $f : \theta \rightarrow \theta'$, on montre

$$\llbracket f \rrbracket_s R_{\theta \rightarrow \theta'} \llbracket f \rrbracket_r \quad (6).$$

15 Il s'ensuit que les deux machines virtuelles sont en relation, c'est-à-dire que :

$$\llbracket \text{état} \rrbracket_s R_{\text{type-état}} \llbracket \text{état} \rrbracket_r \quad (7).$$

20 Comme les relations sont l'identité pour les types observables, les codes source et transformé sont observationnellement identiques.

La dernière étape consiste à montrer qu'il existe un transformateur Γ (figure 1 : 2) qui satisfait les relations logiques. Cela peut être fait en vérifiant qu'un transformateur donné $\Gamma : S \rightarrow T$ satisfait la relation logique associée au type de son argument, avec S code source (figure 1 : 1) et T code transformé
25 (figure 1 : 3). Pour ce faire il est nécessaire qu'il obéisse à la relation suivante :

$$\forall x \llbracket \theta \rrbracket_s . x R_{\theta} \Gamma(x) \quad (8).$$

30 Il vient d'être montré que les relations logiques spécifient un ensemble de contraintes. On peut donc en extraire un transformateur 2 correct par

10

construction, en appliquant des techniques de raffinement ou d'extraction, en faisant appel à un des assistants de preuve appropriés..

Le procédé selon l'invention présente donc un avantage important car il permet une grande mécanisation du processus de vérification, et surtout
5 permet de le conduire à bien, car cette vérification est menée sur des sous-ensembles moins complexes.

Si la transformation du code source 1 peut se décrire comme une succession de transformations plus simples, cette méthode peut s'appliquer pour montrer chaque transformation indépendamment. Il s'ensuit qu'elle
10 présente un grand avantage de modularité.

La vérification ne doit être effectuée que sur les sous-ensembles de fonctions auxiliaires 10 et 30, comme illustré par la figure 2B, à l'aide d'un organe 6, matériel ou logiciel. On a supposé qu'il existe n fonctions auxiliaires, référencées $10_a, 10_b, \dots, 10_i, \dots, 10_{n-1}, 10_n$ et $20_a, 20_b, \dots, 20_i, \dots, 20_{n-1}, 20_n$,
15 respectivement. Si l'organe 6 est matériel, il comporte autant de circuits vérificateurs, $60_a, 60_b, \dots, 60_i, \dots, 60_{n-1}, 60_n$ (représentés arbitrairement sur la figure 2B par le symbole d'un comparateur), que de paires de fonctions auxiliaires à vérifier, par exemple le circuit vérificateur 60_i pour la paire de fonctions 10_i et 30_i . La ou les sortie(s) de cet organe 6, sous la référence
20 unique 61, indique(nt) que la relation logique entre toutes les paires possibles de fonctions auxiliaires correspondantes des codes source 1 et transformé 3 est satisfaite. Cette série d'opérations est suffisante pour apporter la preuve formelle de l'équivalence des deux codes, dans leur globalité.

Il est à noter que le procédé selon l'invention est utilisable aussi bien,
25 *a posteriori*, c'est-à-dire pour vérifier un transformateur existant, qu'*a priori*, comme une aide au développement d'un nouveau transformateur. Elle permet notamment, dans ce dernier cas, d'en déterminer les caractéristiques, pour qu'il fonctionne correctement, en d'autres termes pour que le code transformé qui sera généré par ce transformateur à partir du code source satisfasse l'exigence
30 d'équivalence précitée.

On va maintenant se placer dans le cadre des cartes à puce. La figure 3 illustre schématiquement l'architecture d'une carte à puce, référencée

11

7. On n'a représenté sur cette figure que les éléments essentiels à la bonne compréhension du procédé selon l'invention.

La carte à puce 7 comprend notamment un organe d'entrée-sortie 70 permettant des communications avec le monde extérieur, un premier organe de mémoire 71, fixe ou programmable (de type "ROM", "PROM", "EPROM" ou "EEPROM"), et un organe de mémoire vive 72. La carte à puce 7 comprend enfin un microprocesseur ou un microcontrôleur 73 dialoguant par l'intermédiaire de bus avec les autres composants de la carte à puce 7.

L'architecture logicielle d'une telle carte à puce 7 obéit à la norme ISO 7816-3, se traduisant par une couche protocolaire allant des couches les plus basses associées aux organes d'entrée-sortie 70, jusqu'aux couches les plus hautes associées aux applications logicielles enregistrées dans la carte à puce 7. Ces normes prévoient que les transmissions s'effectuent en mode série.

Le code source 1, une fois transformé par le transformateur de code 2, est transmis à la carte à puce 7 pour y être enregistré, généralement dans l'organe de mémoire 71, fixe ou "semi-fixe", via l'organe d'entrée-sortie 70. La ou les applications logicielles traitées par la carte à puce 7 peuvent être enregistrées à demeure dans la carte à puce 7, c'est-à-dire dans l'organe de mémoire 71, ou de façon transitoire dans la mémoire vive 72. Dans ce dernier cas les applications sont téléchargées via l'organe d'entrée-sortie 70. Dans l'exemple décrit, il a été supposé que la carte à puce 7 est d'un type multi-applications, voire multi-utilisateurs. Il a donc été également supposé que la carte à puce 7 traite m applications logicielles, A_1 à A_m , écrites dans le langage transformé 3.

Un des langages couramment utilisés pour les cartes à puce est, comme il a été rappelé, le langage "Java Card". Il s'agit d'un langage dédié à la programmation des cartes à puce, langage qui constitue une restriction du langage "Java".

La carte 7 peut également stocker un convertisseur supplémentaire effectuant des conversions *in situ* au chargement sur des parties de codes.

12

Les étapes du procédé selon l'invention qui viennent d'être décrites dans un cadre général, vont être illustrées plus particulièrement dans ce cadre d'application préférée.

Comme il est connu, une implantation du langage "Java Card" fait
5 appel à un convertisseur qui transforme des fichiers dits "de classes" en
fichiers "CAP". Un fichier de classe est une unité de compilation et de
représentation du code objet d'un programme "Java". Un fichier CAP regroupe
toutes les classes d'un même "package Java Card" et ne comporte qu'un
unique "constant pool". Un "package Java Card" est une construction "Java"
10 pour regrouper des classes et créer des espaces de noms. Pour sa part, un
"constant pool" est une table associée à chaque fichier de classe pour "Java"
et à chaque fichier "CAP" pour "Java Card". Cette table regroupe des
constantes (chaînes de caractères, entiers, ...). Elle est utilisée dans les
machines virtuelles de "Java" et "Java Card". La transformation est non triviale
15 et globale : elle remplace tous les noms (de packages, de classes, de champs,
de méthodes) par des entités appelées "tokens", c'est-à-dire des nombres
entiers de 7 ou 8 bits. Ces "tokens" servent d'index pour accéder à des tables.
De plus, la transformation regroupe tous les fichiers de classes d'un même
package en un fichier CAP (avec fusion des "constant pools" et réorganisation
20 des tables de méthodes).

Le langage "Java Card" est notamment destiné à être utilisé sur des
cartes à puce bancaires. Il est donc impératif de vérifier la correction de la
transformation d'un programme (ou "byte code") écrit dans la machine virtuelle
du langage "Java" en un programme écrit dans la machine virtuelle du langage
25 "Java Card", c'est-à-dire d'apporter la preuve de l'équivalence de ces deux
programmes.

Cette preuve formelle va être apportée en exécutant les étapes du
procédé selon l'invention.

La première étape consiste en la définition d'une sémantique
30 opérationnelle.

On associe à chaque instruction du "byte code" une ou plusieurs
règles sémantiques. Le "byte code" est un code assembleur portable. C'est le

13

code objet pour les machines virtuelles "Java" ou "Java Card" Par exemple, la règle sémantique associée à l'une des instructions de ce code, l'instruction "getfield" peut se décrire ainsi:

$$\begin{array}{l}
 5 \quad f_ref := \text{constant_pool}(c)(i) \\
 \quad \langle c_ref, iv \rangle := h(\tau) \\
 \quad v := iv(f_ref) \\
 \hline
 10 \quad \langle \text{getfield } i; bc, r :: ops, l, c, h \rangle \Rightarrow \langle bc, v :: ops, 1, c, h \rangle \quad (9).
 \end{array}$$

Dans l'exemple, l'état se compose du code exécuté avec l'instruction courante en tête ($\text{getfield } i; bc$), d'une pile d'opérandes ($r :: ops$), des variables locales (l), d'une référence à la classe courante (c) et du tas (h). La règle spécifie les opérations effectuées lors de l'exécution de $\text{getfield } i$:

- 15 - La fonction auxiliaire "constant_pool" utilise l'index i pour obtenir la référence f_ref du champ (une signature ou un "token", selon qu'il s'agit du code source ou transformé) dans le "constant pool" approprié.
- La référence τ à l'objet dont le champ doit être lu est trouvée en sommet de pile. Cette référence permet de trouver dans le tas ($h(r)$) la classe dynamique de l'objet c_ref (un nom qualifié ou une paire de tokens selon qu'il s'agit du code source ou transformé) et la liste des champs de l'objet (iv).
- 20 - En utilisant la référence précédemment calculée et la liste des champs, le champ est lu ($v := iv(f_ref)$).
- 25 - L'instruction getfield change l'état en remplaçant la référence à l'objet par la valeur du champ et l'exécution se poursuit avec la suite du code (bc).

La deuxième étape consiste en la définition des types.

Dans le cas du langage "Java Card", on définit le type `Word` pour représenter l'unité de stockage :

30

$$\text{Word} = \text{Object_ref} + \text{Null} + \text{Boolean} + \text{Byte} + \text{Short} \quad (10),$$

14

Comme exemple de type construit, le type d'un constant pool est :

$$\text{Constant_pool} = \text{CP_index} \rightarrow \text{CP_info} \quad (11),$$

5 avec :

$$\text{CP_info} = \text{Class_ref} + \text{Method_ref} + \text{Field_ref} \quad (12).$$

10 Dans l'exemple, un "constant pool" est vu comme une fonction prenant un index (le type CP_index est considéré comme basique) et rendant une entrée (ici une référence à une classe, une méthode ou un champ).

Le type du "byte code" est :

$$\begin{aligned} \text{Bytecode} &= \text{Instruction} + \text{Bytecode}; \text{Bytecode} \\ 15 \quad \text{Instruction} &= \text{getfieldCP_index} + \text{Invokevirtual Cp_index} + \dots \quad (13). \end{aligned}$$

Le "byte code" est une séquence d'instructions. Le type Instruction énumère toutes les instructions utilisées dans le "byte code" de "Java Card".

20 La troisième étape consiste en l'interprétation des types

Dans le cas de "Java Card", l'interprétation pour le code source, sous la forme de fichiers de classe (qui utilise des noms), est notée $[[]_{name}$ et l'interprétation pour le code transformé sous la forme de fichiers CAP (qui utilise des "tokens") est notée $[[]_{tok}$.

25 A titre d'exemple, le type $[[\text{CP_index}]_{name}$ est vérifié pour le code source :

$$[[\text{CP_index}]_{name} = \text{Class_name} \times \text{Index} \quad (14).$$

15

Dans le modèle à base de noms, un index de "constant pool" est constitué d'un nom de classe (pour indiquer le "constant pool" auquel on fait référence) et d'un index.

Le type $[[CP_index]]_{tok}$ est vérifié pour le code transformé :

5

$$[[CP_index]]_{tok} = Package_token \times Index \quad (15).$$

Un index de "constant pool" est constitué d'un "token" de "package" (dans l'exemple décrit, il existe un "constant pool" unique par "package" ou fichier CAP) et d'un index.

10

La relation R_{CP_index} est définie comme une bijection telle que : (16)

$$\langle c_name, i \rangle R_{CP_index} \langle p_tok, i' \rangle \Rightarrow pack_name(c_name) R_{package_ref} p_tok$$

15

Le nom du "package" de la classe contenant le "constant pool" auquel il est fait référence dans le modèle à base de noms doit être en relation avec le "token" du "package" contenant le "constant pool" auquel il est fait référence dans le modèle à base de "tokens". La seule contrainte sur les index i et i' est que R_{cp_index} doit être une bijection (les entrées des "constant pools" peuvent donc être regroupées et réordonnées).

20

La quatrième étape consiste en l'interprétation des fonctions auxiliaires

Par exemple, la version de la fonction auxiliaire "constant_pool" pour le modèle à base de noms est :

25

$$[[constant_pool]]_{name} = cp_name \quad (17),$$

avec :

30

$$cp_name\ c = let\ (\dots, cp, \dots) = env_name(pack_name(c))(c) \quad (18).$$

16
in cp

La fonction pack_name prend un nom de classe et rend un nom de "package" et la fonction env_name prend un nom de package et un nom de classe et trouve dans la hiérarchie de classes la structure représentant le
 5 fichier de classe désigné. Le constant pool est extrait du fichier de classe.

Pour le modèle à base de "tokens", la version de la fonction auxiliaire $[[\text{constant_pool}]]_{tok}$ est :

$$10 \quad [[\text{constant_pool}]]_{tok} = \text{cp_tok} \quad (19),$$

avec :

$$15 \quad \text{cp_tok } c = \text{let } (\dots, \text{cp}, \dots) = \text{env_tok}(p) \quad (20). \\ \text{in cp}$$

Le "constant pool" est trouvé dans l'environnement (c'est-à-dire les fichiers CAP) à l'aide de la fonction env_tok et du token de package.

La cinquième étape consiste à prouver que les fonctions auxiliaires
 20 respectent des relations logiques.

Si on se reporte de nouveau à l'exemple de la fonction d'accès au "constant pool", il est nécessaire de déterminer que :

$$25 \quad [[\text{constant_pool}]]_{name} R_{cp_index \rightarrow CP_info} [[\text{constant_pool}]]_{tok} \quad (21).$$

La relation $R_{cp_index \rightarrow CP_info}$ est complètement définie en fonction des relations R_{CP_index} et R_{CP_info} . En se servant de cette définition, on montre qu'il suffit de vérifier que :

$$30 \quad \forall (c_name, i)(p_tok, i') \text{ tels que } \langle c_name, i \rangle R_{CP_index} \langle p_tok, i' \rangle \\ \text{cp}(i) R_{CP_info} \text{cp}'(i') \quad (22),$$

avec :

$$\begin{aligned}
 & (\dots, cp, \dots) = \text{env_name}(\text{pack_name}(c_name))(c_name) \\
 5 \quad & (\dots, cp', \dots) = \text{env_tok}(p_tok)
 \end{aligned} \tag{23}$$

La preuve se fonde sur la définition de R_{CP_info} et la propriété rappelée ci-dessus : (24)

$$10 \quad (c_name, i) R_{cp_index} (p_tok, i') \Rightarrow \text{pack_name}(c_name) R_{package_ref} p_tok$$

La sixième et dernière étape du procédé consiste à déterminer un transformateur tel que la transformation du code et des données par ce convertisseur respecte des relations logiques déterminées. Par exemple, les
 15 références à des "packages" sont, soit des noms, soit des "tokens" suivant le modèle. La relation logique associée $R_{package_ref}$ est définie simplement comme une bijection entre les noms de "package" et les "tokens" de "package". Il suffit de vérifier que la fonction du convertisseur réalisant la transformation des noms de package en "tokens" est effectivement une bijection.

20 A la lecture de ce qui précède, on constate aisément que l'invention atteint bien les buts qu'elle s'est fixés.

Il doit être clair cependant que l'invention n'est pas limitée aux seuls exemples de réalisations explicitement décrits, notamment en relation avec les figures 2 et 3.

25 Enfin, bien que le procédé ait été décrit de façon détaillée dans le cas de la transformation d'un programme de la machine virtuelle du langage "Java" en un programme de la machine virtuelle du langage "Java Card", particulièrement intéressant pour les applications de type carte à puce ou similaire, l'invention n'est en aucun cas limitée à cette application particulière.

30 L'invention peut trouver application à chaque fois que le dispositif impliqué ne dispose que de ressources informatiques relativement limitées, notamment en ce qui concerne la capacité mémoire (vive ou fixe) et/ou la

18

puissance de calcul du processeur utilisé. On peut citer à titre d'exemple des livres électroniques, par exemple du type dit "e-book", destinés à télécharger et stocker des données en provenance de sites Internet, des calculateurs de poche, par exemple du type dit "organiser", certains téléphones mobiles

5 pouvant être connectés au réseau Internet, etc. Dans tous ces cas, il est nécessaire de disposer d'un langage optimisé pour utiliser au mieux les ressources informatiques intégrées.

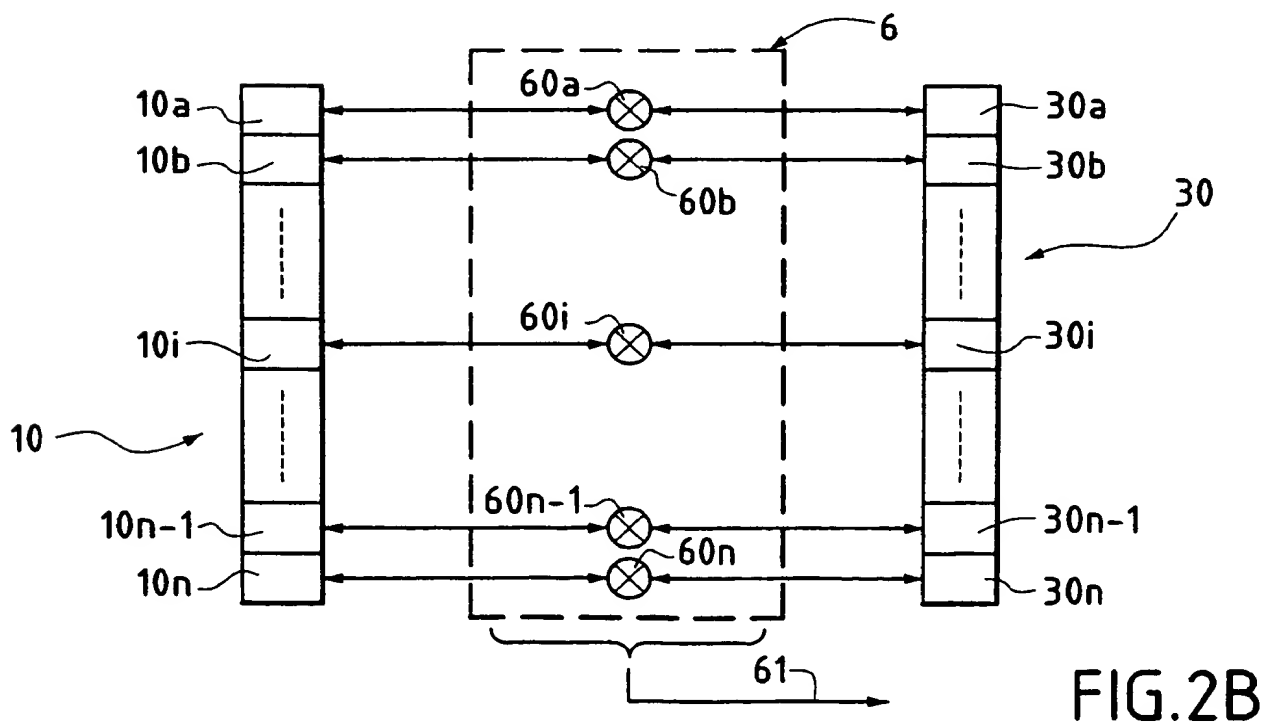
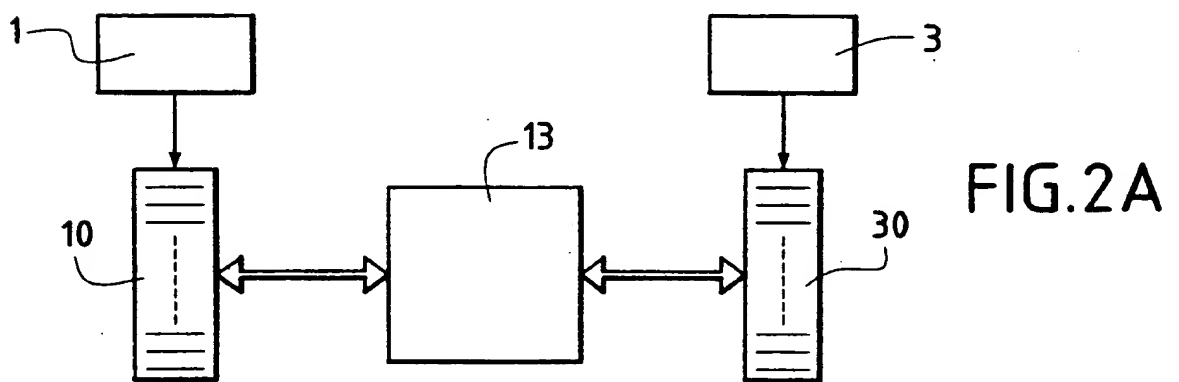
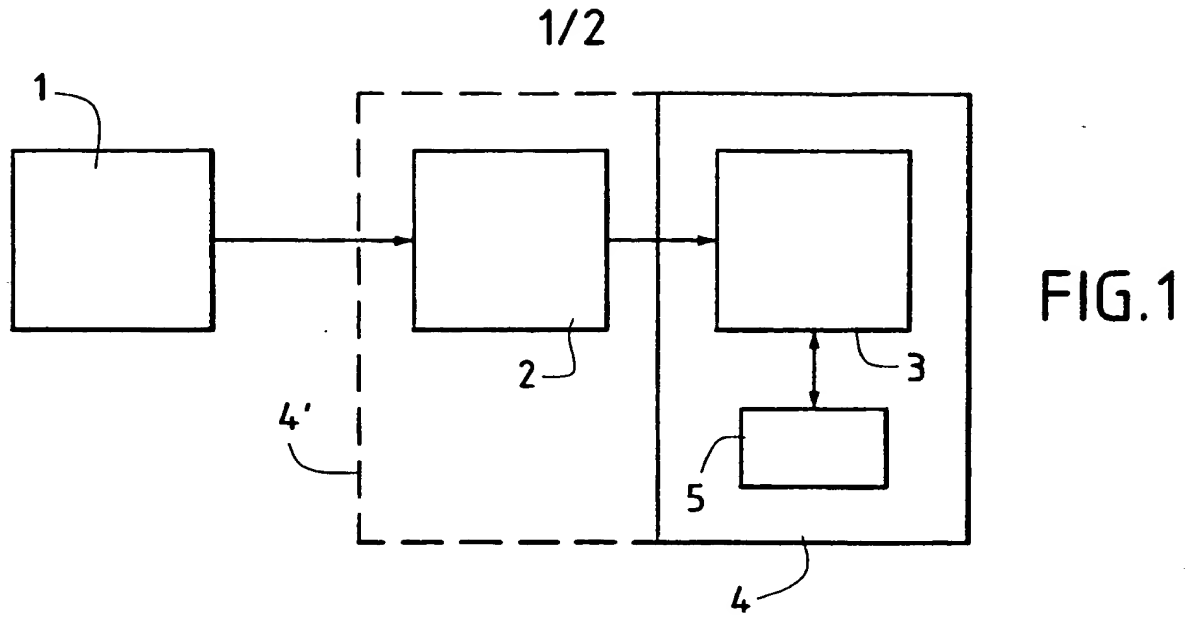
REVENDICATIONS

1. Procédé de vérification d'un transformateur de code dit source en un code dit transformé destiné à un système embarqué, lesdits codes source et transformé étant associés à des machines virtuelles, caractérisé en ce qu'il comprend au moins les étapes suivantes :
- la détermination, pour chacun desdits codes source (1) et transformé (3), d'un premier sous-ensemble (13) commun constituant une machine virtuelle unique factorisant le comportement de ces deux codes (1, 3) ;
 - la détermination, pour chacun desdits codes source (1) et transformé (3), d'un second sous-ensemble (10, 30) constitué d'une pluralité de fonctions dites auxiliaires (10_i - 30_i) utilisées par ladite machine virtuelle unique, lesdites fonctions auxiliaires (10_i - 30_i) représentant des différences résiduelles entre lesdits codes source (1) et transformé (3) ;
 - l'association par paire desdites fonctions auxiliaires, une première fonction auxiliaire (10_i) de chaque paire appartenant audit second sous-ensemble (10) associé audit code source (1) et une seconde fonction auxiliaire (30_i) de chaque paire appartenant audit second sous-ensemble (30) associé audit code transformé (3) ;
 - la vérification (6) d'une propriété de correspondance déterminée entre lesdites fonctions auxiliaires de toutes lesdites paires (10_i - 30_i) ; et
 - la vérification que ladite transformation du code source (1) en code transformé (3) par ledit convertisseur (2) respecte ladite propriété de correspondance déterminée.
2. Procédé selon la revendication 1, caractérisé en ce que ladite propriété de correspondance est une relation logique, de manière à ce que lesdites fonctions auxiliaires de chacune desdites paires (10_i - 30_i), lors de leur exécution, génèrent des résultats liés par ladite relation logique, et en ce que cette relation est la relation identité pour des entités dites observables

20

de chacun desdits codes, source et transformé, pour toute paire de fonctions auxiliaires, de manière à ce que les fonctionnalités dudit code source (1) soient préservées lors de ladite transformation dans ledit code transformé (3), et ladite vérification de transformateur de code (2) réalisée.

- 5 3. Application du procédé de vérification selon l'une des revendications 1 ou 2 à un transformateur de code (2) générant, à partir dudit code source (1) un code transformé (3) destiné à être enregistré dans des moyens de mémoire (71) d'une carte à puce (7).
- 10 4. Application selon la revendication 3, caractérisé en ce que, ledit code transformé étant un programme écrit dans la machine virtuelle d'un langage informatique déterminé, ladite carte à puce (7) est une carte à puce enregistrant une pluralité d'applications logicielles (A_1 à A_n) écrites dans ce code transformé (3).
- 15 5. Application selon les revendications 3 ou 4, caractérisé en ce que ledit code source (1) est un programme écrit dans la machine virtuelle du langage "JAVA" (marque déposée) et ledit code transformé (3) est un programme écrit dans la machine virtuelle du langage "JAVA CARD" (marque déposée).



This Page Blank (uspto)

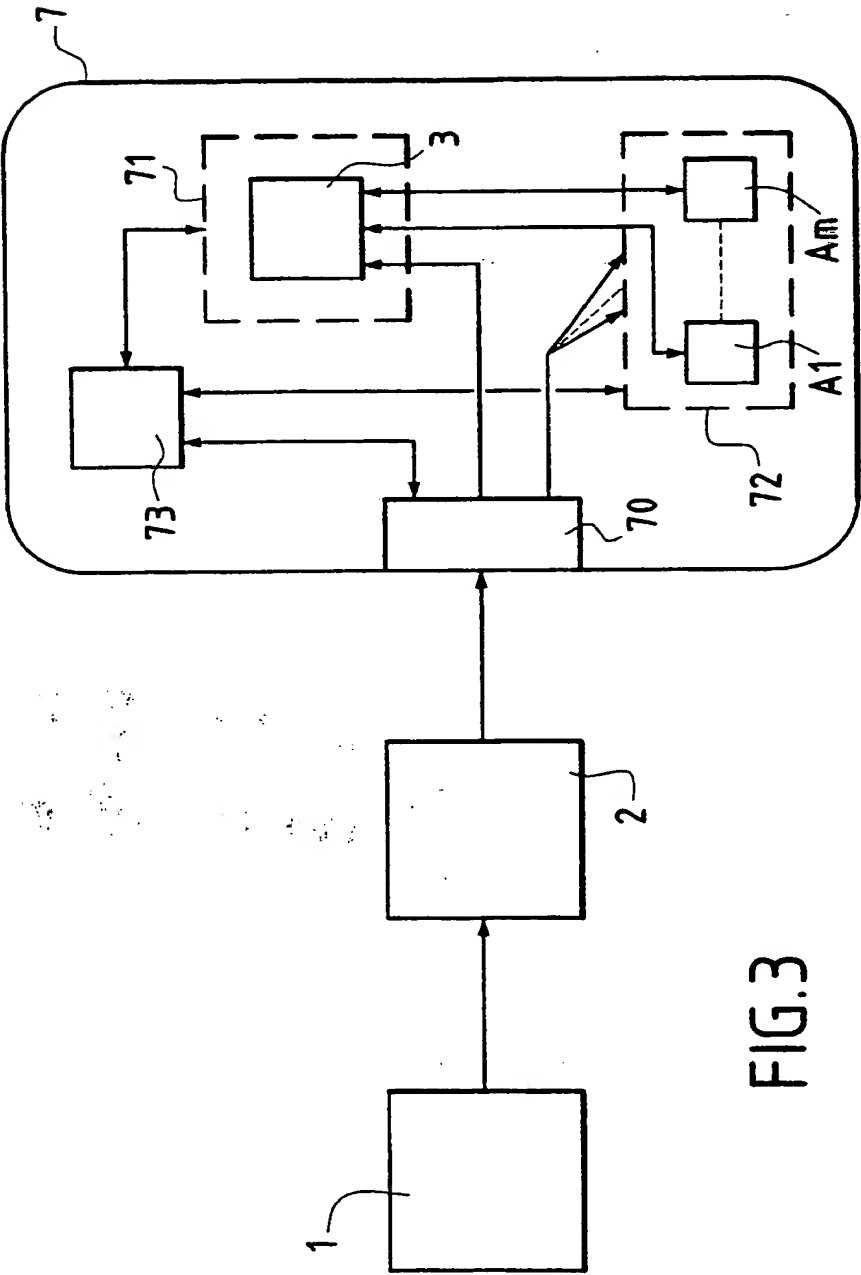


FIG.3

This Page Blank (uspto)

PCT

REQUETE

Le soussigné requiert que la présente demande internationale soit traitée conformément au Traité de coopération en matière de brevets.

Réservé à l'office récepteur

Demande internationale n°

Date du dépôt international

Nom de l'office récepteur et "Demande internationale PCT"

Référence du dossier du déposant ou du mandataire (facultatif)
(12 caractères au maximum) JLB51856

Cadre n° I TITRE DE L'INVENTION

Procédé de vérification de transformateurs de codage pour un système embarqué, notamment sur une carte à puce.

Cadre n° II DEPOSANT

Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)

DULL CP0
68 Route de Versailles
78430 LOUVECIENNES
FRANCE

☐ Cette personne est aussi inventeur.

n° de téléphone

n° de télécopieur

n° de téléimprimeur

Nationalité (nom de l'Etat) : FRANCE

Domicile (nom de l'Etat) : FRANCE

Cette personne est
déposant pour :

☐ tous les Etats
désignés

☒ tous les Etats désignés sauf
les Etats-Unis d'Amérique

☐ les Etats-Unis d'Amérique
seulement

☐ les Etats indiqués dans
le cadre supplémentaire

Cadre n° III AUTRE(S) DEPOSANT(S) OU (AUTRE(S)) INVENTEUR(S)

Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)

Institut National de la Recherche en Informatique et en Automatique
Domaine de Voluceau
Rocquencourt
F-78153 LE CHESNAY CEDEX
FRANCE

Cette personne est :

☒ déposant seulement

☐ déposant et inventeur

☐ inventeur seulement
(Si cette case est cochée,
ne pas remplir la suite.)

Nationalité (nom de l'Etat) : FRANCE

Domicile (nom de l'Etat) : FRANCE

Cette personne est
déposant pour :

☐ tous les Etats
désignés

☒ tous les Etats désignés sauf
les Etats-Unis d'Amérique

☐ les Etats-Unis d'Amérique
seulement

☐ les Etats indiqués dans
le cadre supplémentaire

☒ D'autres déposants ou inventeurs sont indiqués sur une feuille annexée.

Cadre n° IV MANDATAIRE OU REPRESENTANT COMMUN; OU ADRESSE POUR LA CORRESPONDANCE

La personne dont l'identité est donnée ci-dessous est/la été désignée pour agir au nom du ou des déposants auprès des autorités internationales compétentes, comme :

☒ mandataire

☐ représentant commun

Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays.)

Georges ROGER PETIT, c/o OFFICE RI FTRY
2, bd de Strasbourg
F-75010 PARIS - FRANCE

n° de téléphone

01 42 08 39 58

n° de télécopieur

01 53 38 43 14

n° de téléimprimeur

☐ Adresse pour la correspondance: cocher cette case lorsque aucun mandataire ni représentant commun n'est/n'a été désigné et que l'espace ci-dessus est utilisé pour indiquer une adresse spéciale à laquelle la correspondance doit être envoyée.

This Page Blank (uspto)

Feuille n° 2.....

Suite du cadre n° III AUTRES DEPOSANTS OU (AUTRES) INVENTEURS	
Si aucun des sous-cadres suivants n'est utilisé, cette feuille ne doit pas être incluse dans la requête.	
<p>Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)</p> <p>Le Centre National de la Recherche Scientifique (CNRS) 3 rue Michel-Ange F-75194 PARIS CEDEX 16 FRANCE</p>	<p>Cette personne est :</p> <p><input checked="" type="checkbox"/> déposant seulement</p> <p><input type="checkbox"/> déposant et inventeur</p> <p><input type="checkbox"/> inventeur seulement (Si cette case est cochée, ne pas remplir la suite.)</p>
Nationalité (nom de l'Etat) : FRANCE	Domicile (nom de l'Etat) : FRANCE
<p>Cette personne est déposant pour :</p> <p><input type="checkbox"/> tous les Etats désignés <input checked="" type="checkbox"/> tous les Etats désignés sauf les Etats-Unis d'Amérique <input type="checkbox"/> les Etats-Unis d'Amérique seulement <input type="checkbox"/> les Etats indiqués dans le cadre supplémentaire</p>	
<p>Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)</p> <p>GOIRE Christian 8 Allée du Mail F-70340 LES CLAYES SOUS BOIS FRANCE</p>	<p>Cette personne est :</p> <p><input type="checkbox"/> déposant seulement</p> <p><input checked="" type="checkbox"/> déposant et inventeur</p> <p><input type="checkbox"/> inventeur seulement (Si cette case est cochée, ne pas remplir la suite.)</p>
Nationalité (nom de l'Etat) : FRANCE	Domicile (nom de l'Etat) : FRANCE
<p>Cette personne est déposant pour :</p> <p><input type="checkbox"/> tous les Etats désignés <input type="checkbox"/> tous les Etats désignés sauf les Etats-Unis d'Amérique <input checked="" type="checkbox"/> les Etats-Unis d'Amérique seulement <input type="checkbox"/> les Etats indiqués dans le cadre supplémentaire</p>	
<p>Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)</p> <p>JENSEN Thomas IRISA/INRIA Campus Universitaire de Beaulieu F-35042 RENNES CEDEX FRANCE</p>	<p>Cette personne est :</p> <p><input type="checkbox"/> déposant seulement</p> <p><input checked="" type="checkbox"/> déposant et inventeur</p> <p><input type="checkbox"/> inventeur seulement (Si cette case est cochée, ne pas remplir la suite.)</p>
Nationalité (nom de l'Etat) : FRANCE	Domicile (nom de l'Etat) : FRANCE
<p>Cette personne est déposant pour :</p> <p><input type="checkbox"/> tous les Etats désignés <input type="checkbox"/> tous les Etats désignés sauf les Etats-Unis d'Amérique <input checked="" type="checkbox"/> les Etats-Unis d'Amérique seulement <input type="checkbox"/> les Etats indiqués dans le cadre supplémentaire</p>	
<p>Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)</p> <p>FRADET Pascal IRISA/INRIA Campus Universitaire de Beaulieu F-35042 RENNES CEDEX FRANCE</p>	<p>Cette personne est :</p> <p><input type="checkbox"/> déposant seulement</p> <p><input checked="" type="checkbox"/> déposant et inventeur</p> <p><input type="checkbox"/> inventeur seulement (Si cette case est cochée, ne pas remplir la suite.)</p>
Nationalité (nom de l'Etat) : FRANCE	Domicile (nom de l'Etat) : FRANCE
<p>Cette personne est déposant pour :</p> <p><input type="checkbox"/> tous les Etats désignés <input type="checkbox"/> tous les Etats désignés sauf les Etats-Unis d'Amérique <input checked="" type="checkbox"/> les Etats-Unis d'Amérique seulement <input type="checkbox"/> les Etats indiqués dans le cadre supplémentaire</p>	
<p><input checked="" type="checkbox"/> D'autres déposants ou inventeurs sont indiqués sur une autre feuille annexe</p>	

This Page Blank (uspto)

Feuille n° 3

Cadre supplémentaire. Si le cadre supplémentaire n'est pas utilisé, cette feuille ne doit pas être incluse dans la requête.

1. Si l'un des cadres du présent formulaire ne suffit pas à contenir tous les renseignements : dans ce cas, indiquer "Suite du cadre n° ..." (préciser le numéro du cadre) et fournir les renseignements conformément aux instructions données dans le cadre dans lequel la place était insuffisante, en particulier :

- i) si plus de deux personnes sont en cause comme déposants ou inventeurs et que l'on ne dispose d'aucune "feuille annexe" : dans ce cas, indiquer "Suite du cadre n° III" et fournir pour chaque personne supplémentaire le même type de renseignements que ceux qui sont demandés dans le cadre n° III. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous;
- ii) si, dans le cadre n° II ou dans l'un des sous-cadres du cadre n° III, la case "les Etats indiqués dans le cadre supplémentaire" est cochée : dans ce cas, indiquer "Suite du cadre n° II" ou "Suite du cadre n° III" ou "Suite des cadres n° II et III" (selon le cas), ainsi que le nom du ou des déposants en cause et, à côté de chaque nom, le ou les Etats pour lesquels la personne mentionnée a la qualité de déposant (ou, le cas échéant, la mention "brevet ARIPO", "brevet eurasiatique", "brevet européen" ou "brevet OAPI") ;
- iii) si, dans le cadre n° II ou dans l'un des sous-cadres du cadre n° III, l'inventeur ou l'inventeur/déposant n'a pas la qualité d'inventeur pour tous les Etats désignés ou pour les Etats-Unis d'Amérique : dans ce cas, indiquer "Suite du cadre n° II" ou "Suite des cadres n° II et III" (selon le cas), ainsi que le nom du ou des inventeurs et, à côté de chaque nom, le ou les Etats pour lesquels la personne mentionnée a la qualité d'inventeur (ou, le cas échéant, la mention "brevet ARIPO", "brevet eurasiatique", "brevet européen" ou "brevet OAPI") ;
- iv) si, en plus du ou des mandataires indiqués dans le cadre n° IV, il y a d'autres mandataires : dans ce cas, indiquer "Suite du cadre n° IV" et fournir pour chaque mandataire supplémentaire le même type de renseignements que ceux qui sont demandés dans le cadre n° IV ;
- v) si, dans le cadre n° V, le nom d'un Etat (ou de l'OAPI) est assorti de la mention "brevet d'addition" ou "certificat d'addition" ou si, dans le cadre n° VI le nom des Etats-Unis d'Amérique est assorti de la mention "continuation" ou "continuation-in-part" : dans ce cas, indiquer "Suite du cadre n° V" ainsi que le nom de chaque Etat en cause (ou de l'OAPI) en précisant après chaque nom le numéro du titre principal ou de la demande principale ainsi que la date de délivrance du titre principal ou la date de dépôt de la demande principale ;
- vi) si, dans le cadre n° VI, la priorité de plus de trois demandes antérieures est revendiquée : dans ce cas, indiquer "Suite du cadre n° VI" et fournir pour chaque demande antérieure supplémentaire le même type de renseignements que ceux qui sont demandés dans le cadre n° VI ;
- vii) si, dans le cadre n° VI, la demande antérieure est une demande ARIPO : dans ce cas, indiquer "Suite du cadre n° VI", préciser le point correspondant à cette demande antérieure et indiquer au moins un pays partie à la Convention de Paris pour la protection de la propriété industrielle pour lequel cette demande antérieure a été déposée.

2. Si, en ce qui concerne la déclaration concernant les désignations de précaution contenue dans le cadre n° V, le déposant souhaite exclure un ou plusieurs Etats de la portée de cette déclaration : dans ce cas, indiquer "Designations exclues de la portée de la déclaration concernant les désignations de précaution" et fournir le nom ou le code à deux lettres de chaque Etat concerné.

3. Si le déposant revendique, à l'égard d'un office désigné, le bénéfice de dispositions de la législation nationale concernant des divulgations non opposables ou des exceptions au défaut de nouveauté : dans ce cas, indiquer "Déclaration concernant des divulgations non opposables ou des exceptions au défaut de nouveauté" et rédiger au dessous cette déclaration.

"Suite du cadre n° III"

- LE METAYER Daniel
IRISA/INRIA
Campus Universitaire de Beaulieu
F- 35042 RENNES CEDEX
FRANCE

Nationalité (nom de l'Etat) : FRANCE

Domicile (nom de l'Etat) : FRANCE

Cette personne est : déposant et inventeur.

Cette personne est déposant pour : les Etats-Unis d'Amérique seulement.

- DENNEY Ewen
IRISA/INRIA
Campus Universitaire de Beaulieu
F- 35042 RENNES CEDEX
FRANCE

Nationalité (nom de l'Etat) : FRANCE

Domicile (nom de l'Etat) : FRANCE

Cette personne est : déposant et inventeur.

Cette personne est déposant pour : les Etats-Unis d'Amérique seulement

This Page Blank (uspto)

Feuille n° 4

Cadre n° V DESIGNATION D'ÉTATS

Les désignations suivantes sont faites conformément à la règle 4.9.b) (recher les cases appropriées; une au moins doit l'être):

Brevet régional

- ☐ AP Brevet AKIPO : GH Ghana, GM Gambie, KE Kenya, LS Lesotho, MW Malawi, SD Soudan, SL Sierra Leone, SZ Swaziland, UG Ouganda, ZW Zimbabwe et tout autre État qui est un État contractant du Protocole de Harare et du PCT
- ☐ EA Brevet eurasien : AM Arménie, AZ Azerbaïdjan, BY Bélarus, KG Kirghizistan, KZ Kazakhstan, MD République de Moldova, RU Fédération de Russie, TJ Tadjikistan, TM Turkménistan et tout autre État qui est un État contractant de la Convention sur le brevet eurasien et du PCT
- ☒ EP Brevet européen : AT Autriche, BE Belgique, CH et LI Suisse et Liechtenstein, CY Chypre, DE Allemagne, DK Danemark, ES Espagne, FI Finlande, FR France, GB Royaume-Uni, GR Grèce, IE Irlande, IT Italie, LU Luxembourg, MC Monaco, NL Pays-Bas, PT Portugal, SE Suède et tout autre État qui est un État contractant de la Convention sur le brevet européen et du PCT
- ☐ OA Brevet OAPI : BF Burkina Faso, BJ Bénin, CF République centrafricaine, CG Congo, CI Côte d'Ivoire, CM Cameroun, GA Gabon, GN Guinée, GW Guinée-Bissau, ML Mali, MR Mauritanie, NE Niger, SN Sénégal, TD Tchad, TG Togo et tout autre État qui est un État membre de l'OAPI et un État contractant du PCT (si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée).

Brevet national (si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée):

- | | |
|--|---|
| <input type="checkbox"/> AE Émirats arabes unis | <input type="checkbox"/> LR Libéria |
| <input type="checkbox"/> AL Albanie | <input type="checkbox"/> LS Lesotho |
| <input type="checkbox"/> AM Arménie | <input type="checkbox"/> LT Lituanie |
| <input type="checkbox"/> AT Autriche | <input type="checkbox"/> LU Luxembourg |
| <input type="checkbox"/> AU Australie | <input type="checkbox"/> LV Lettonie |
| <input type="checkbox"/> AZ Azerbaïdjan | <input type="checkbox"/> MD République de Moldova |
| <input type="checkbox"/> BA Bosnie-Herzégovine | <input type="checkbox"/> MC Madagascar |
| <input type="checkbox"/> BB Barbade | <input type="checkbox"/> MK Ex-République yougoslave de Macédoine |
| <input type="checkbox"/> BG Bulgarie | |
| <input checked="" type="checkbox"/> BR Brésil | <input type="checkbox"/> MN Mongolie |
| <input type="checkbox"/> BY Bélarus | <input type="checkbox"/> MW Malawi |
| <input checked="" type="checkbox"/> CA Canada | <input type="checkbox"/> MX Mexique |
| <input type="checkbox"/> CH et LI Suisse et Liechtenstein | <input type="checkbox"/> NO Norvège |
| <input checked="" type="checkbox"/> CN Chine | <input type="checkbox"/> NZ Nouvelle-Zélande |
| <input type="checkbox"/> CU Cuba | <input type="checkbox"/> PL Pologne |
| <input type="checkbox"/> CZ République tchèque | <input type="checkbox"/> PT Portugal |
| <input type="checkbox"/> DE Allemagne | <input type="checkbox"/> RO Roumanie |
| <input type="checkbox"/> DK Danemark | <input type="checkbox"/> RU Fédération de Russie |
| <input type="checkbox"/> EE Estonie | <input type="checkbox"/> SD Soudan |
| <input type="checkbox"/> ES Espagne | <input type="checkbox"/> SE Suède |
| <input type="checkbox"/> FI Finlande | <input type="checkbox"/> SC Singapour |
| <input type="checkbox"/> GB Royaume-Uni | <input type="checkbox"/> SI Slovénie |
| <input type="checkbox"/> GD Grenade | <input type="checkbox"/> SK Slovaquie |
| <input type="checkbox"/> GE Géorgie | <input type="checkbox"/> SL Sierra Leone |
| <input type="checkbox"/> GH Ghana | <input type="checkbox"/> TJ Tadjikistan |
| <input type="checkbox"/> GM Gambie | <input type="checkbox"/> TM Turkménistan |
| <input type="checkbox"/> HR Croatie | <input type="checkbox"/> TR Turquie |
| <input type="checkbox"/> HU Hongrie | <input type="checkbox"/> TT Trinité-et-Tobago |
| <input type="checkbox"/> ID Indonésie | <input type="checkbox"/> UA Ukraine |
| <input type="checkbox"/> IL Israël | <input type="checkbox"/> UG Ouganda |
| <input type="checkbox"/> IN Inde | <input checked="" type="checkbox"/> US États-Unis d'Amérique |
| <input type="checkbox"/> IS Islande | |
| <input checked="" type="checkbox"/> JP Japon | <input type="checkbox"/> UZ Ouzbékistan |
| <input type="checkbox"/> KE Kenya | <input type="checkbox"/> VN Viet Nam |
| <input type="checkbox"/> KG Kirghizistan | <input type="checkbox"/> YU Yougoslavie |
| <input type="checkbox"/> KP République populaire démocratique de Corée | <input type="checkbox"/> ZA Afrique du Sud |
| <input type="checkbox"/> KR République de Corée | <input type="checkbox"/> ZW Zimbabwe |
| <input type="checkbox"/> KZ Kazakhstan | |
| <input type="checkbox"/> LC Sainte-Lucie | |
| <input type="checkbox"/> LK Sri Lanka | |

Cases réservées pour la désignation d'États qui sont devenus parties au PCT après la publication de la présente feuille.

Déclaration concernant les désignations de protection: outre les désignations faites ci-dessus, le déposant fait aussi conformément à la règle 4.9.b) toutes les désignations qui seraient autorisées en vertu du PCT, à l'exception de toute désignation indiquée dans le cadre supplémentaire comme étant exclue de la portée de cette déclaration. Le déposant déclare que ces désignations additionnelles sont faites sous réserve de confirmation et que toute désignation qui n'est pas confirmée avant l'expiration d'un délai de 15 mois à compter de la date de priorité doit être considérée comme retirée par le déposant à l'expiration de ce délai. (Pour confirmer une désignation, il faut déposer une déclaration contenant la désignation en question et payer les taxes de désignation et de confirmation. La confirmation doit parvenir à l'office récepteur dans le délai de 3 mois.)

Formulaire PCT/RO/101 (deuxième feuille) (juillet 1999)

Voir les notes relatives au formulaire de requête

This Page Blank (uspto)

Feuille n° 5

Cadre n° VI REVENDEICATION DE PRIORITE				
Date de dépôt de la demande antérieure (jour/mois/année)	Numéro de la demande antérieure	Lorsque la demande antérieure est une :		
		demande nationale : pays	demande régionale :* office régional	demande internationale : office récepteur
(1) (1er Juillet 1999) 01/07/1999	9908160	FRANCE		
(2)				
(3)				

☒ L'office récepteur est prié de préparer et de transmettre au Bureau international une copie certifiée conforme de la ou des demandes antérieures (seulement si la demande antérieure a été déposée auprès de l'office qui, aux fins de la présente demande internationale, est l'office récepteur) indiquées ci-dessous au(x) point(s) : (1)

* Si la demande antérieure est une demande ARIPO, il est obligatoire d'indiquer dans le cadre supplémentaire au moins un pays partie à la Convention de Furt pour la protection de la propriété industrielle pour lequel cette demande antérieure a été déposée (règle 4.10.b.iii). Voir le cadre supplémentaire.

Cadre n° VII ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE	
Choix de l'administration chargée de la recherche internationale (ISA) (si plusieurs administrations chargées de la recherche internationale sont compétentes pour procéder à la recherche internationale, indiquer l'administration choisie; le code à deux lettres pour être utilisé) : ISA / OFB	Demande d'utilisation des résultats d'une recherche antérieure; mention de cette recherche (si une recherche antérieure a été effectuée par l'administration chargée de la recherche internationale ou demandée à cette dernière) : Date (jour/mois/année) Numéro Pays (ou office régional)

Cadre n° VIII BORDEREAU; LANGUE DE DÉPÔT	
La présente demande internationale contient le nombre de feuilles suivant :	Le ou les éléments cochés ci après sont joints à la présente demande internationale :
requête : 5	1. <input checked="" type="checkbox"/> feuille de calcul des taxes
description (sauf partie réservée au listage des séquences) : 10	2. <input type="checkbox"/> pouvoir distinctif signé
revendications : 2	3. <input type="checkbox"/> copie du pouvoir général; numéro de référence, le cas échéant :
abrégé : 1	4. <input type="checkbox"/> explication de l'absence d'une signature
dessins : 2	5. <input type="checkbox"/> document(s) de priorité indiqué(s) dans le cadre n° VI au(x) point(s) : (1)
partie de la description réservée au listage des séquences : —	6. <input type="checkbox"/> traduction de la demande internationale en (langue) :
Nombre total de feuilles : 28	7. <input type="checkbox"/> indications séparées concernant des micro-organismes ou autre matériel biologique déposés
Figure des dessins qui doit accompagner l'abrégé : 3	8. <input type="checkbox"/> listage des séquences de nucléotides ou d'acides aminés sous forme déchiffrable par ordinateur
	9. <input type="checkbox"/> autres éléments (produit) :
	Langue de dépôt de la demande internationale : Française

Cadre n° IX SIGNATURE DU DEPOSANT OU DU MANDATAIRE	
A côté de chaque signature, indiquer le nom du signataire et, si celui-ci n'apparaît pas clairement à la lecture de la requête, à quel titre l'intéressé signe.	
Georges ROGER-PETIT	
mandataire	

Réservé à l'office récepteur	
1. Date effective de réception des pièces supposées constituer la demande internationale :	2. Dessins : <input type="checkbox"/> reçus : <input type="checkbox"/> non reçus :
3. Date effective de réception, rectifiée en raison de la réception ultérieure, mais dans les délais, de documents ou de dessins complétant ce qui est supposé constituer la demande internationale :	
4. Date de réception, dans les délais, des corrections demandées selon l'article 11.2 du PCT :	
5. Administration chargée de la recherche internationale (si plusieurs sont compétentes) : ISA /	
6. <input type="checkbox"/> Transmission de la copie de recherche différée jusqu'au paiement de la taxe de recherche.	

Réservé au Bureau international	
Date de réception de l'exemplaire original par le Bureau international :	

Formulaire PCT/RO/101 (dernière feuille) (juillet 1998; réimpression juillet 1999) Voir les notes relatives au formulaire de requête

mis Page Blank (uspto)

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 00/01815

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06F9/45

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F G06N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, INSPEC, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KAUFMANN M ET AL: "AN INDUSTRIAL STRENGTH THEOREM PROVER FOR A LOGIC BASED ON COMMON LISP" IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, US, IEEE INC. NEW YORK, vol. 23, no. 4, 1 April 1997 (1997-04-01), pages 203-213, XP000720014 ISSN: 0098-5589 the whole document	1,2
A	FR 2 757 970 A (GEMPLUS CARD INT) 3 July 1998 (1998-07-03) claims 1,6,7	1,4

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *G* document member of the same patent family

Date of the actual completion of the international search

1 September 2000

Date of mailing of the international search report

08/09/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Kingma, Y

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 00/01815

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>ALBERDA M I ET AL: "Using formal methods to cultivate trust in smart card operating systems"</p> <p>FUTURE GENERATIONS COMPUTER SYSTEMS,NL,ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM,</p> <p>vol. 13, no. 1, 1 July 1997 (1997-07-01), pages 39-54, XP004081708</p> <p>ISSN: 0167-739X</p> <p>page 53, left-hand column, line 2 - line 33</p> <p>abstract</p> <p style="text-align: center;">-----</p>	1-4

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 00/01815

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2757970 A	03-07-1998	AU 5769598 A	31-07-1998
		CN 1247609 A	15-03-2000
		EP 1012710 A	28-06-2000
		WO 9829803 A	09-07-1998
<hr/>			

This Page Blank (uspto)

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire JL/B51856	POUR SUITE A DONNER voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 00/ 01815	Date du dépôt international(jour/mois/année) 28/06/2000	(Date de priorité (la plus ancienne) (jour/mois/année) 01/07/1999
Déposant BULL CP8		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

☒ Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. Base du rapport

- a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.
- ☐ la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.
- b. En ce qui concerne les **séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :
- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposée avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. ☐ Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (voir le cadre I).

3. ☐ Il y a absence d'unité de l'invention (voir le cadre II).

4. En ce qui concerne le titre,

- ☒ le texte est approuvé tel qu'il a été remis par le déposant.
- ☐ Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'abrégé,

- ☒ le texte est approuvé tel qu'il a été remis par le déposant
- ☐ le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure des dessins à publier avec l'abrégé est la Figure n°

- ☒ suggérée par le déposant.
- ☐ parce que le déposant n'a pas suggéré de figure.
- ☐ parce que cette figure caractérise mieux l'invention.

3

☐ Aucune des figures n'est à publier.

This Page Blank (uspto)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No

CT/FR 00/01815

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F9/45

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 G06F G06N

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

EPO-Internal, INSPEC, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	KAUFMANN M ET AL: "AN INDUSTRIAL STRENGTH THEOREM PROVER FOR A LOGIC BASED ON COMMON LISP" IEEE TRANSACTIONS ON SOFTWARE ENGINEERING,US,IEEE INC. NEW YORK, vol. 23, no. 4, 1 avril 1997 (1997-04-01), pages 203-213, XP000720014 ISSN: 0098-5589 le document en entier ----	1,2
A	FR 2 757 970 A (GEMPLUS CARD INT) 3 juillet 1998 (1998-07-03) revendications 1,6,7 ----- -/--	1,4

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

- *A* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- *E* document antérieur, mais publié à la date de dépôt international ou après cette date
- *L* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- *O* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- *P* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- *T* document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- *X* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- *Y* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- *&* document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

1 septembre 2000

Date d'expédition du présent rapport de recherche internationale

08/09/2000

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Kingma, Y

Page Blank (uspto)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>ALBERDA M I ET AL: "Using formal methods to cultivate trust in smart card operating systems"</p> <p>FUTURE GENERATIONS COMPUTER SYSTEMS,NL,ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, vol. 13, no. 1, 1 juillet 1997 (1997-07-01), pages 39-54, XP004081708</p> <p>ISSN: 0167-739X</p> <p>page 53, colonne de gauche, ligne 2 - ligne 33</p> <p>abrégé</p> <p>-----</p>	1-4

This Page Blank (uspto)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 00/01815

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
FR 2757970	A	03-07-1998	AU 5769598 A	31-07-1998
			CN 1247609 A	15-03-2000
			EP 1012710 A	28-06-2000
			WO 9829803 A	09-07-1998

uge Blank (uspto)

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

NOTIFICATION DE LA RECEPTION DE
L'EXEMPLAIRE ORIGINAL

(règle 24.2.a) du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

ROGER PETIT, Georges
Office Blety
2, boulevard de Strasbourg
F-75010 Paris
FRANCE

Date d'expédition (jour/mois/année) 29 août 2000 (29.08.00)	NOTIFICATION IMPORTANTE
Référence du dossier du déposant ou du mandataire JL/B51856	Demande internationale no PCT/FR00/01815

Il est notifié au déposant que le Bureau international a reçu l'exemplaire original de la demande internationale précisée ci-après.

Nom(s) du ou des déposants et de l'Etat ou des Etats pour lesquels ils sont déposants:

BULL CP8 etc. (pour tous les Etats désignés sauf US)
GOIRE, Christian etc. (pour US seulement)

Date du dépôt international : 28 juin 2000 (28.06.00)
Date(s) de priorité revendiquée(s) : 01 juillet 1999 (01.07.99)
Date de réception de l'exemplaire original par le Bureau international : 02 août 2000 (02.08.00)
Liste des offices désignés :

EP : AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE
National : BR, CA, CN, JP, US

ATTENTION

Le déposant doit soigneusement vérifier les indications figurant dans la présente notification. En cas de divergence entre ces indications et celles que contient la demande internationale, il doit aviser immédiatement le Bureau international.

En outre, l'attention du déposant est appelée sur les renseignements donnés dans l'annexe en ce qui concerne

- ☒ les délais dans lesquels doit être abordée la phase nationale
- ☒ la confirmation des désignations faites par mesure de précaution
- ☐ les exigences relatives aux documents de priorité.

Une copie de la présente notification est envoyée à l'office récepteur et à l'administration chargée de la recherche internationale.

Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse	Fonctionnaire autorisé Philippe Bécamel
n° de télécopieur (41-22) 740.14.35	n° de téléphone (41-22) 338.83.38

Page blank (uspto)

ANNEXE DU FORMULAIRE PCT/IB/301

Demande internationale no
PCT/FR00/01815RENSEIGNEMENTS CONCERNANT LES DELAIS DANS LESQUELS DOIT ETRE ABORDEE
LA PHASE NATIONALE

Il est rappelé au déposant qu'il doit aborder la "phase nationale" auprès de chacun des offices désignés indiqués sur la notification de la réception de l'exemplaire original (formulaire PCT/IB/301) en payant les taxes nationales et en remettant les traductions, telles qu'elles sont prescrites par les législations nationales.

Le délai d'accomplissement de ces actes de procédure est de 20 MOIS à compter de la date de priorité ou, pour les Etats désignés qui ont été élus par le déposant dans une demande d'examen préliminaire international ou dans une élection ultérieure, de 30 MOIS à compter de la date de priorité, à condition que cette élection ait été effectuée avant l'expiration du 19e mois à compter de la date de priorité. Certains offices désignés (ou élus) ont fixé des délais qui expirent au-delà de 20 ou 30 mois à compter de la date de priorité. D'autres offices accordent une prolongation des délais ou un délai de grâce, dans certains cas moyennant le paiement d'une taxe supplémentaire.

En plus de ces actes de procédure, le déposant devra dans certains cas satisfaire à d'autres exigences particulières applicables dans certains offices. Il appartient au déposant de veiller à remplir en temps voulu les conditions requises pour l'ouverture de la phase nationale. La majorité des offices désignés n'envoient pas de rappel à l'approche de la date limite pour aborder la phase nationale.

Des informations détaillées concernant les actes de procédure à accomplir pour aborder la phase nationale auprès de chaque office désigné, les délais applicables et la possibilité d'obtenir une prolongation des délais ou un délai de grâce et toutes autres conditions applicables figurent dans le volume II du Guide du déposant du PCT. Les exigences concernant le dépôt d'une demande d'examen préliminaire international sont exposées dans le chapitre IX du volume I du Guide du déposant du PCT.

GR et ES sont devenues liées par le chapitre II du PCT le 7 septembre 1996 et le 6 septembre 1997, respectivement, et peuvent donc être élues dans une demande d'examen préliminaire international ou dans une élection ultérieure présentée le 7 septembre 1996 (ou à une date postérieure) ou le 6 septembre 1997 (ou à une date postérieure), respectivement, quelle que soit la date de dépôt de la demande internationale (voir le second paragraphe, ci-dessus).

Veuillez noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

CONFIRMATION DES DESIGNATIONS FAITES PAR MESURE DE PRECAUTION

Seules les désignations expresses faites dans la requête conformément à la règle 4.9.a) figurent dans la présente notification. Il est important de vérifier si ces désignations ont été faites correctement. Des erreurs dans les désignations peuvent être corrigées lorsque des désignations ont été faites par mesure de précaution en vertu de la règle 4.9.b). Toute désignation ainsi faite peut être confirmée conformément aux dispositions de la règle 4.9.c) avant l'expiration d'un délai de 15 mois à compter de la date de priorité. En l'absence de confirmation, une désignation faite par mesure de précaution sera considérée comme retirée par le déposant. Il ne sera adressé aucun rappel ni invitation. Pour confirmer une désignation, il faut déposer une déclaration précisant l'Etat désigné concerné (avec l'indication de la forme de protection ou de traitement souhaitée) et payer les taxes de désignation et de confirmation. La confirmation doit parvenir à l'office récepteur dans le délai de 16 mois.

EXIGENCES RELATIVES AUX DOCUMENTS DE PRIORITE

Pour les déposants qui n'ont pas encore satisfait aux exigences relatives aux documents de priorité, il est rappelé ce qui suit.

Lorsque la priorité d'une demande nationale, régionale ou internationale antérieure est revendiquée, le déposant doit présenter une copie de cette demande antérieure, certifiée conforme par l'administration auprès de laquelle elle a été déposée ("document de priorité"), à l'office récepteur (qui la transmettra au Bureau international) ou directement au Bureau international, avant l'expiration d'un délai de 16 mois à compter de la date de priorité, étant entendu que tout document de priorité peut être présenté au Bureau international avant la date de publication de la demande internationale, auquel cas ce document sera réputé avoir été reçu par le Bureau international le dernier jour du délai de 16 mois (règle 17.1.a)).

Lorsque le document de priorité est délivré par l'office récepteur, le déposant peut, au lieu de présenter ce document, demander à l'office récepteur de le préparer et de le transmettre au Bureau international. La requête à cet effet doit être formulée avant l'expiration du délai de 16 mois et peut être soumise au paiement d'une taxe (règle 17.1.b)).

Si le document de priorité en question n'est pas fourni au Bureau international, ou si la demande adressée à l'office récepteur de préparer et de transmettre le document de priorité n'a pas été faite (et la taxe correspondante acquittée, le cas échéant) avant l'expiration du délai applicable mentionné aux paragraphes précédents, tout Etat désigné peut ne pas tenir compte de la revendication de priorité; toutefois, aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.

Lorsque plusieurs priorités sont revendiquées, la date de priorité à prendre en considération aux fins du calcul du délai de 16 mois est la date du dépôt de la demande la plus ancienne dont la priorité est revendiquée.

This Page Blank (uspto)

TRAITÉ DE COOPERATION EN MATIÈRE DE BREVETS

PCT

AVIS INFORMANT LE DEPOSANT DE LA
COMMUNICATION DE LA DEMANDE
INTERNATIONALE AUX OFFICES DESIGNES

(règle 47.1.c), première phrase, du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

ROGER PETIT, Georges
Office Bletry
94, rue Saint Lazare
F-75010 Paris
FRANCE

Date d'expédition (jour/mois/année) 11 janvier 2001 (11.01.01)		
Référence du dossier du déposant ou du mandataire JL/B51856		AVIS IMPORTANT
Demande internationale no PCT/FR00/01815	Date du dépôt international (jour/mois/année) 20 juin 2000 (20.06.00)	Date de priorité (jour/mois/année) 01 juillet 1999 (01.07.99)
Déposant BULL CP8 etc		

1. Il est notifié par la présente qu'à la date indiquée ci-dessus comme date d'expédition de cet avis, le Bureau international a communiqué, comme le prévoit l'article 20, la demande internationale aux offices désignés suivants:

US

Conformément à la règle 47.1.c), troisième phrase, ces offices acceptent le présent avis comme preuve déterminante du fait que la communication de la demande internationale a bien eu lieu à la date d'expédition indiquée plus haut, et le déposant n'est pas tenu de remettre de copie de la demande internationale à l'office ou aux offices désignés.

2. Les offices désignés suivants ont renoncé à l'exigence selon laquelle cette communication doit être effectuée à cette date:

BR,CA,CN,EP,JP

La communication sera effectuée seulement sur demande de ces offices. De plus, le déposant n'est pas tenu de remettre de copie de la demande internationale aux offices en question (règle 49.1)a-bis)).

3. Le présent avis est accompagné d'une copie de la demande internationale publiée par le Bureau international le 11 janvier 2001 (11.01.01) sous le numéro WO 01/02955

RAPPEL CONCERNANT LE CHAPITRE II (article 31.2)a) et règle 54.2)

Si le déposant souhaite reporter l'ouverture de la phase nationale jusqu'à 30 mois (ou plus pour ce qui concerne certains offices) à compter de la date de priorité, la demande d'examen préliminaire international doit être présentée à l'administration compétente chargée de l'examen préliminaire international avant l'expiration d'un délai de 19 mois à compter de la date de priorité.

Il appartient exclusivement au déposant de veiller au respect du délai de 19 mois.

Il est à noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

RAPPEL CONCERNANT L'OUVERTURE DE LA PHASE NATIONALE (article 22 ou 39.1))

Si le déposant souhaite que la demande internationale procède en phase nationale, il doit, dans le délai de 20 mois ou de 30 mois, ou plus pour ce qui concerne certains offices, accomplir les actes mentionnés dans ces dispositions auprès de chaque office désigné ou élu.

Pour d'autres informations importantes concernant les délais et les actes à accomplir pour l'ouverture de la phase nationale, voir l'annexe du formulaire PCT/IB/301 (Notification de la réception de l'exemplaire original) et le volume II du Guide du déposant du PCT.

Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse	Fonctionnaire autorisé J. Zahra
no de télécopieur (41 22) 740.14.36	no de téléphone (41-22) 338.83.38

This Page blank (uspto)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☒ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (usp10)